

Further Results on Homogeneous Two-Weight Codes

Thomas Honold

ABSTRACT. The results of [1, 2] on linear homogeneous two-weight codes over finite Frobenius rings are extended in two ways: It is shown that certain non-projective two-weight codes give rise to strongly regular graphs in the way described in [1, 2]. Secondly, these codes are used to define a dual two-weight code and strongly regular graph similar to the classical case of projective linear two-weight codes over finite fields [3].

1. Introduction

A finite ring R is said to be a Frobenius ring if there exists a character $\chi \in \widehat{R} = \text{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$ whose kernel contains no nonzero left (or right) ideal of R . The (normalized) homogeneous weight $w_{\text{hom}}: R \rightarrow \mathbb{C}$ on a finite Frobenius ring R is defined by

$$w_{\text{hom}}(x) = 1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(ux). \quad (1)$$

(This does not depend on the choice of χ .) The function w_{hom} is the unique complex-valued function on R satisfying $w_{\text{hom}}(0) = 0$, $w_{\text{hom}}(ux) = w_{\text{hom}}(x)$ for $x \in R$, $u \in R^\times$ and $\sum_{x \in I} w_{\text{hom}}(x) = |I|$ for all nonzero left ideals $I \leq_R R$ (and their right counterparts).

The homogeneous weight on a finite Frobenius ring is a generalization of both the Hamming weight on \mathbb{F}_q ($w_{\text{hom}}(x) = \frac{q}{q-1} w_{\text{Ham}}(x)$ for $x \in \mathbb{F}_q$) and the Lee weight on \mathbb{Z}_4 ($w_{\text{hom}}(x) = w_{\text{Lee}}(x)$ for $x \in \mathbb{Z}_4$). It was introduced in [4] for the case $R = \mathbb{Z}_m$ and generalized to Frobenius rings in [6, 8].

2000 *Mathematics Subject Classification.* Primary 94B05; Secondary 05E30, 05B10.

Key words and phrases. Codes over Frobenius rings, homogeneous weight, two-weight code, modular code, strongly regular graph, partial difference set.

Reprint of the conference paper published in the Proceedings of the Fifth International Workshop on Optimal Codes and Related Topics (OC2007), White Lagoon, Bulgaria, June 2007, pp. 80–86.

In [1, 2] it was shown that a linear code C over a finite Frobenius ring with exactly two nonzero homogeneous weights and satisfying certain nondegeneracy conditions gives rise to a strongly regular graph with C as its set of vertices. In the classical case $R = \mathbb{F}_q$ this result has been known for a long time and forms part of a more general correspondence between projective linear $[n, k]$ two-weight codes over \mathbb{F}_q and certain strongly regular Cayley graphs of $(\mathbb{F}_q^k, +)$ resp. regular partial difference sets in $(\mathbb{F}_q^k, +)$, and their (appropriately defined) duals (cf. [3, 5]).

The purpose of this work is to generalize the results of [1, 2] to a larger class of homogeneous two-weight codes (so-called modular two-weight codes) and establish for these codes the classical correspondence (Theorems 3.2 and 5.7 of [3]) in full generality.

2. A Few Properties of Frobenius Rings and their Homogeneous Weights

For a subset S of a ring R let ${}^\perp S = \{x \in R; xS = 0\}$, $S^\perp = \{x \in R; Sx = 0\}$. Similarly, for $S \subseteq R^n$ let ${}^\perp S = \{\mathbf{x} \in R^n; \mathbf{x} \cdot S = 0\}$ and $S^\perp = \{\mathbf{x} \in R^n; S \cdot \mathbf{x} = 0\}$, where $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$.

PROPOSITION 1. *A finite ring R is a Frobenius ring iff for every matrix $\mathbf{A} \in R^{m \times n}$ the left row space $C = \{\mathbf{x}\mathbf{A}; \mathbf{x} \in R^m\}$ and the right column space $D = \{\mathbf{A}\mathbf{y}; \mathbf{y} \in R^n\}$ have the same cardinality.*

From now on we suppose that R is a finite Frobenius ring with homogeneous weight w_{hom} .

First we determine the set of all $x \in R$ satisfying $w_{\text{hom}}(x) = 0$. Let $S_i = Rs_i$, $1 \leq i \leq \tau$, be the different left ideals of R of order 2 and $S = S_1 + \cdots + S_\tau$. The set S is a two-sided ideal of R of order 2^τ , whose elements are the subset sums of $\{s_1, \dots, s_\tau\}$. Define $S_0 \subseteq S$ as the set of all sums of an even number of elements from $\{s_1, \dots, s_\tau\}$ (“even-weight subcode of S ”). Note that S_0 is a subgroup of $(R, +)$, trivial for $\tau \leq 1$ and nontrivial (of order $2^{\tau-1}$) for $\tau \geq 2$.

PROPOSITION 2. *We have $w_{\text{hom}}(x) \geq 0$ for all $x \in R$, and $\{x \in R; w_{\text{hom}}(x) = 0\} = S_0$. Moreover, $w_{\text{hom}}(x + y) = w_{\text{hom}}(x)$ for all $x \in R$ and $y \in S_0$.*

FACT 3 ([7, Th. 2]).

$$\sum_{x \in I} w_{\text{hom}}(x + c) = |I| \quad (2)$$

for all nonzero left (or right) ideals I of R and all $c \in R$.

The following correlation property of w_{hom} turns out to be crucial.

PROPOSITION 4. For a nonzero left ideal I of R and $r, s \in R$ we have

$$\sum_{x \in I} w_{\text{hom}}(x) w_{\text{hom}}(xr + s) = \begin{cases} |I| + |I| \cdot \frac{|R^\times \cap (1+I^\perp)|}{|R^\times|} \cdot (1 - w_{\text{hom}}(s)) & \text{if } |Ir| = |I|, \\ |I| & \text{if } |Ir| < |I|. \end{cases} \quad (3)$$

In particular $\sum_{x \in R} w_{\text{hom}}(x)^2 = |R| + \frac{|R|}{|R^\times|}$.

For vectors $\mathbf{x}, \mathbf{y} \in R^k$ we write $\mathbf{x} \sim \mathbf{y}$ if $\mathbf{x}R^\times = \mathbf{y}R^\times$. By [10, Prop. 5.1] this is equivalent to $\mathbf{x}R = \mathbf{y}R$.

PROPOSITION 5. For nonzero words $\mathbf{g}, \mathbf{h} \in R^k$ and $s \in R$ we have

$$\sum_{\mathbf{x} \in R^k} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}) w_{\text{hom}}(\mathbf{x} \cdot \mathbf{h} + s) = \begin{cases} |R|^k + \frac{|R|^k}{|\mathbf{g}R^\times|} \cdot (1 - w_{\text{hom}}(s)) & \text{if } \mathbf{g} \sim \mathbf{h}, \\ |R|^k & \text{if } \mathbf{g} \not\sim \mathbf{h}. \end{cases} \quad (4)$$

3. Modular Two-Weight Codes, Partial Difference Sets and Strongly Regular Cayley Graphs

Given a positive integer k , the set of nonzero cyclic submodules of the free right module R_R^k is denoted by \mathcal{P} . The elements of \mathcal{P} are referred to as *points* of the projective geometry $\text{PG}(R_R^k)$, and a multiset $\alpha: \mathcal{P} \rightarrow \mathbb{N}_0$ is referred to as a *multiset in $\text{PG}(R_R^k)$* .

With a left linear code $C \leq {}_R R^n$ generated by k (or fewer) codewords and having no all-zero coordinate we associate a multiset α_C in $\text{PG}(R_R^k)$ of cardinality n in the following way: If $C = \{\mathbf{x}\mathbf{G}; \mathbf{x} \in R^k\}$ with $\mathbf{G} = (\mathbf{g}_1 | \mathbf{g}_2 | \dots | \mathbf{g}_n) \in R^{k \times n}$, define $\alpha_C: \mathcal{P} \rightarrow \mathbb{N}_0$ by $\alpha(\mathbf{g}R) = |\{j; 1 \leq j \leq n \wedge \mathbf{g}_j R = \mathbf{g}R\}|$. The relation $C \leftrightarrow \alpha_C$ defines a bijection between classes of monomially isomorphic left linear codes over R generated by k codewords and orbits of the group $\text{GL}(R_R^k)$ on multisets in $\text{PG}(R_R^k)$.

DEFINITION 6. A linear code $C \leq {}_R R^n$ is said to be *modular* if there exists $r \in \mathbb{Q}$ such that for all points $\mathbf{g}R$ of $\text{PG}(R_R^k)$ either $\alpha_C(\mathbf{g}R) = 0$ or $\alpha_C(\mathbf{g}R) = r|\mathbf{g}R^\times|$. The number r is called the *index* of C .

The property of C described in Def. 6 does not depend on the choice of α_C (not even on the dimension k). Hence modularity of a linear code is a well-defined concept.

If $A \subseteq R^k \setminus \{\mathbf{0}\}$ satisfies $AR^\times = A$, the matrix \mathbf{G} with the vectors of A as columns generates a modular (left) linear code of length $|A|$ and index 1.

Note that projective codes over \mathbb{F}_q are modular of index $\frac{1}{q-1}$ and regular projective codes over R as defined in [1, 2] are modular of index $\frac{1}{|R^\times|}$.

FACT 7 ([11, Th. 5.4]). A linear code $C \leq_R R^n$ is a one-weight code (i. e. equidistant w. r. t. w_{hom}) iff C is modular and $\{\mathbf{g} \in R^k \setminus \{\mathbf{0}\}; \alpha_C(\mathbf{g}R) > 0\}$ is the set of nonzero vectors of a submodule of R_R^k .

The main purpose of this paper is a combinatorial characterization of linear homogeneous two-weight codes over R , i. e. linear codes over R having exactly two nonzero homogeneous weights $w_1 < w_2$. Assuming that C is such a code, we set $w_0 = 0$, $C_i = \{\mathbf{c} \in C; w_{\text{hom}}(\mathbf{c}) = w_i\}$ and $b_i = |C_i|$ for $i = 0, 1, 2$.

By Prop. 2 we have $w_{\text{hom}}(\mathbf{c}) = 0$ iff $w_{\text{hom}}(c_j) = 0$ for $1 \leq j \leq n$, the set C_0 is a subgroup of $(C, +)$ and C_1, C_2 are unions of cosets of C_0 . If the weights w_1, w_2 and $b_0 = |C_0|$ are known, the frequencies b_1, b_2 can be computed from the equations $b_1 + b_2 = |C| - |C_0|$, $b_1 w_1 + b_2 w_2 = \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) = n|C|$ (assuming that C has no all-zero coordinate) and are given by

$$b_1 = \frac{(w_2 - n)|C| - w_2|C_0|}{w_2 - w_1}, \quad b_2 = \frac{(n - w_1)|C| + w_1|C_0|}{w_2 - w_1}. \quad (5)$$

LEMMA 8. For a modular code $C \leq_R R^n$ of index r and $\mathbf{d} \in R^n$ we have

$$\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(\mathbf{c} + \mathbf{d}) = |C| \cdot (n^2 + rn - r \cdot w_{\text{hom}}(\mathbf{d})). \quad (6)$$

In the special case $\mathbf{d} = \mathbf{0}$ Lemma 8 reduces to $\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c})^2 = (n^2 + rn)|C|$.

LEMMA 9. The nonzero weights w_1, w_2 of a modular two-weight code $C \leq_R R^n$ of index r satisfy the relation

$$(w_1 + w_2)n|C| = (n^2 + rn)|C| + w_1 w_2(|C| - |C_0|). \quad (7)$$

LEMMA 10. For a modular two-weight code $C \leq_R R^n$ of index r and $\mathbf{d} \in R^n$ we have

$$\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) = b_1 w_1 + \left(b_1 - \frac{b_1 w_1}{n}\right) w_{\text{hom}}(\mathbf{d}) \quad (8)$$

REMARK 11. Lemmas 8 and 10 can be generalized to

$$\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(c_j + d_j) = |C| \cdot (n + r - r \cdot w_{\text{hom}}(d_j)) \quad \text{and}$$

$$\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(c_j + d_j) = \frac{b_1 w_1}{n} + \left(b_1 - \frac{b_1 w_1}{n}\right) w_{\text{hom}}(d_j)$$

respectively, where j is any coordinate of R^n and $d_j \in R$. In particular $\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(c_j) = \frac{b_1 w_1}{n}$ is independent of j .

Recall that a (simple) graph Γ is *strongly regular with parameters* (N, K, λ, μ) if Γ has N vertices, is regular of degree K and any two adjacent (resp. non-adjacent) vertices have λ (resp. μ) common neighbours. The graph Γ is called

trivial if Γ or its complement is a disjoint union of cliques of the same size. This is equivalent to $\mu = 0$ resp. $\mu = K$.

A subset $D \subset G$ of an (additively written) abelian group G is said to be a *regular* (N, K, λ, μ) *partial difference set in* G if $N = |G|$, $K = |D|$, $0 \notin D$, $-D = D$, and the multiset $D - D$ represents each element of D exactly λ times and each element of $G \setminus (D \cup \{0\})$ exactly μ times; cf. [9].

If D is a regular (N, K, λ, μ) partial difference set in G , then the graph $\Gamma(G, D)$ with vertex set G and edge set $\{\{x, x + d\}; x \in G, d \in D\}$, the so-called *Cayley graph* of G w.r.t. D , is strongly regular with parameters (N, K, λ, μ) .

We are now ready to generalize the main result of [2, 1] to modular two-weight codes. For a two-weight code C we denote the Cayley graph $\Gamma(C/C_0, C_1/C_0)$ by $\Gamma(C)$. Thus the vertices of $\Gamma(C)$ are the cosets of C_0 in C , and two cosets $\mathbf{c} + C_0, \mathbf{d} + C_0$ are adjacent iff $w_{\text{hom}}(\mathbf{c} - \mathbf{d}) = w_1$. As we have already mentioned, Prop. 2 ensures that $\Gamma(C)$ is well-defined.

THEOREM 12. *The graph $\Gamma(C)$ associated with a modular two-weight code over a finite Frobenius ring R is strongly regular with parameters*

$$N = \frac{|C|}{|C_0|}, \quad K = \frac{(w_2 - n)N - w_2}{w_2 - w_1},$$

$$\lambda = \frac{K \left(\frac{w_1^2}{n} - 2w_1 \right) + w_2(K - 1)}{w_2 - w_1}, \quad \mu = \frac{K \left(\frac{w_1 w_2}{n} - w_1 - w_2 \right) + w_2 K}{w_2 - w_1}.$$

The graph $\Gamma(C)$ is trivial iff $w_1 = n$.

REMARK 13. Since $\Gamma(C)$ is a Cayley graph, the preceding argument shows that $\Gamma(C)$ is trivial iff the codewords of weight 0 and w_2 form a linear subcode of C (and the cocliques of $\Gamma(C)$ are the cosets of $(C_0 + C_2)/C_0$ in this case).

4. The Dual of a Modular Two-Weight Code

Suppose $C \leq {}_R R^n$ is a two-weight code over a finite Frobenius ring with nonzero weights $w_1 < w_2$ and frequencies b_1, b_2 . Let $\mathbf{M}_i \in R^{b_i \times n}$ ($i = 1, 2$) be matrices whose rows are the codewords of C of weight w_i in some order.

DEFINITION 14. The right linear code $C' \leq R_R^{b_1}$ generated by the columns of \mathbf{M}_1 is called the *dual of the two-weight code* C .

The code C' is modular of index 1 (no matter whether C is modular or not).

THEOREM 15. *If $C \leq {}_R R^n$ is a modular two-weight code with $C_0 = \{\mathbf{0}\}$, its dual C' is also a (modular) two-weight code with $C'_0 = \{\mathbf{0}\}$ and nonzero weights*

$$w'_1 = \frac{(w_2 - n - r)|C|}{w_2 - w_1} = \frac{b_1 w_1}{n}, \quad w'_2 = \frac{(w_2 - n)|C|}{w_2 - w_1}. \quad (9)$$

THEOREM 16. *Under the assumptions of Th. 15, the graph $\Gamma(C')$ is strongly regular with parameters*

$$N' = |C|, \quad K' = \frac{n}{r}, \quad \lambda' = \frac{2n - w_1 - w_2}{r} + \frac{w_1 w_2}{r^2 |C|}, \quad \mu' = \frac{w_1 w_2}{r^2 |C|}.$$

The graph $\Gamma(C')$ is trivial iff $w_1 = n$ (i. e. iff $\Gamma(C)$ is trivial).

THEOREM 17. *Let $C \leq_R R^n$ be a modular linear code over a finite Frobenius ring R generated by $\mathbf{G} = (\mathbf{g}_1 | \dots | \mathbf{g}_n) \in R^{k \times n}$. Let $D \leq R_R^k$ be the right column space of \mathbf{G} . Suppose C has no all-zero coordinate and satisfies $C_0 = \{\mathbf{0}\}$. Then the following are equivalent:*

- (i) *C is a homogeneous two-weight code;*
- (ii) *$\Omega = \mathbf{g}_1 R^\times \cup \dots \cup \mathbf{g}_n R^\times$ is a regular partial difference set in $(D, +)$ and $\Omega \cup \{\mathbf{0}\}$ is not a submodule of R_R^k .*

REMARK 18. Under the assumptions of Th. 17 the set $\Omega \cup \{\mathbf{0}\}$ is a submodule of R_R^k iff C is a homogeneous one-weight code, and $D \setminus \Omega$ is a submodule of R_R^k iff C is a homogeneous two-weight code with $w_1 = n$.

References

- [1] E. Byrne, M. Greferath, and T. Honold. Two-weight codes over finite Frobenius rings and strongly regular graphs. In *Optimal Codes and Related Topics*, pages 64–73, Pamporovo, Bulgaria, 2005.
- [2] E. Byrne, M. Greferath, and T. Honold. Ring geometries, two-weight codes, and strongly regular graphs. *Designs, Codes and Cryptography*, 48:1–16, July 2008.
- [3] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18:97–122, 1986.
- [4] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problems of Information Transmission*, 33(3):208–213, 1997.
- [5] P. Delsarte. Weights of linear codes and strongly regular normed spaces. *Discrete Mathematics*, 3:47–64, 1972.
- [6] M. Greferath and S. E. Schmidt. Finite-ring combinatorics and MacWilliams’ equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92:17–28, 2000.
- [7] W. Heise and T. Honold. Homogeneous and egalitarian weights on finite rings. In *Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-2000)*, pages 183–188, Bansko, Bulgaria, 2000.
- [8] T. Honold and A. A. Nechaev. Weighted modules and representations of codes. *Problems of Information Transmission*, 35(3):205–223, 1999.
- [9] S. L. Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, 4:221–261, 1994.
- [10] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3):555–575, 1999.
- [11] J. A. Wood. The structure of linear codes of constant weight. *Transactions of the American Mathematical Society*, 354:1007–1026, 2001.

THOMAS HONOLD, INSTITUTE OF INFORMATION AND COMMUNICATION ENGINEERING, ZHE-
JIANG UNIVERSITY, ZHEDA ROAD, 310027 HANGZHOU, CHINA

E-mail address: `honold@zju.edu.cn`